

We claim:

sub
a1
1 1. A method for generating a cryptographic key using at least one parameter
2 comprising the steps of:
3 retrieving at least one cryptographic share from a memory location identified as a
4 function of said at least one parameter; and
5 generating a cryptographic key based on said at least one cryptographic share.

1 2. The method of claim 1 wherein said at least one retrieved cryptographic share
2 is encrypted, said method further comprising the step of:
3 decrypting said at least one cryptographic share.

1 3. The method of claim 2 wherein said step of decrypting comprises the step of:
2 decrypting using a value computed as a function of said at least one parameter.

1 4. The method of claim 1 wherein said at least one retrieved cryptographic share
2 is compressed, said method further comprising the step of:
3 decompressing said at least one cryptographic share.

1 5. The method of claim 4 wherein said step of decompressing comprises the step
2 of:
3 decompressing said at least one cryptographic share using an index of said
4 memory location.

1 6. The method of claim 1 wherein said at least one parameter represents at least
2 one measurement of a physical property.

1 7. The method of claim 1 further comprising the step of:
2 generating at least one index as a function of said at least one parameter; and
3 using said index to identify said memory location.

1 8. The method of claim 7 further comprising the step of:
2 retrieving a cryptographic share from a memory location in the vicinity of said
3 memory location identified by said index.

1 9. The method of claim 7 wherein said step of generating at least one index
2 comprises the step of generating the same index for a set of parameter values.

1 10. The method of claim 9 wherein said set of parameter values are within a
2 predetermined range of values.

1 11. A data structure comprising:
2 a plurality of storage locations;
3 a first subset of said plurality of storage locations containing valid cryptographic
4 shares; and
5 a second subset of said plurality of storage locations containing invalid
6 cryptographic shares.

1 12. The data structure of claim 11 wherein said first subset of storage
2 locations correspond to storage locations which are expected to be accessed during a
3 legitimate computer resource access attempt.

1 13. The data structure of claim 11 wherein said second subset of storage location
2 correspond to storage locations which are expected to be accessed during an illegitimate
3 computer resource access attempt.

1 14. The data structure of claim 11 wherein at least some of said cryptographic
2 shares are encrypted.

1 15. The data structure of claim 14 wherein said encrypted cryptographic shares
2 are encrypted with a password.

1 16. The data structure of claim 11 wherein at least some of said cryptographic
2 shares are compressed.

1 17. The data structure of claim 11 wherein said cryptographic shares are
2 cryptographic shares of a polynomial secret sharing scheme.

1 18. The data structure of claim 11 wherein said cryptographic shares are
2 cryptographic shares of a vector space secret sharing scheme.

1 19. A method for maintaining a data structure which has valid cryptographic
2 shares stored in a plurality of locations, said method comprising the step of:
3 periodically changing the number of locations that contain valid cryptographic
4 shares.

1 20. The method of claim 19 wherein said step of changing the number of
2 locations that contain valid cryptographic shares comprises the step of:
3 storing invalid cryptographic shares in at least some locations which previously
4 contained valid cryptographic shares.

1 21. The method of claim 20 further comprising the step of:
2 storing said invalid cryptographic shares in locations which are not expected to be
3 accessed in connection with an authorized computer resource access attempt.

1 22. The method of claim 19 wherein said step of changing the number of
2 locations that contain valid cryptographic shares comprises the step of:
3 storing valid cryptographic shares in at least some locations which previously
4 contained invalid cryptographic shares.

1 23. The method of claim 22 further comprising the step of:
2 storing said valid cryptographic shares in locations which are expected to be
3 accessed in connection with an authorized computer resource access attempt.

1 24. A method for generating a cryptographic key comprising the steps of:
2 measuring a plurality of keystroke features during entry of a password;
3 retrieving from a data structure a plurality of cryptographic shares as a function of
4 said plurality of keystroke features; and
5 generating a cryptographic key using said cryptographic shares.

1 25. The method of claim 24 wherein said cryptographic shares represent points
2 on a polynomial.

1 26. The method of claim 24 wherein said cryptographic shares represent vectors.

1 27. The method of claim 24 wherein said cryptographic shares are compressed.

1 28. The method of claim 27 wherein said cryptographic shares comprise y values
2 of points on a polynomial and the corresponding x values are derivable from a data
3 structure location.

1 29. The method of claim 24 further comprising the step of:
2 generating a plurality of indices as a function of said keystroke features; and
3 using said plurality of indices to identify locations within said data structure from
4 which to retrieve said cryptographic shares.

1 30. The method of claim 29 wherein said step of generating a plurality of indices
2 as a function of said keystroke features comprises the step of:

3 for each of said keystroke features, generating one of two indices as a function of
4 a threshold value.

1 31. The method of claim 29 wherein said step of generating a plurality of indices
2 as a function of said keystroke features comprises the step of:

3 for each of said keystroke features, generating one of a plurality of indices as a
4 function of a plurality of threshold values.

1 32. The method of claim 24 wherein said cryptographic shares stored in said data
2 structure are encrypted, said method further comprising the step of:

3 decrypting said cryptographic shares using said password.

1 33. The method of claim 24 further comprising the steps of:

2 maintaining a history file containing information relating to prior successful key
3 generation attempts; and

4 based on said history file, storing invalid cryptographic shares in data structure
5 locations which are not expected to be accessed during subsequent legitimate key
6 generation attempts.

1 34. A method for generating a cryptographic key using a plurality of parameters
2 having a sequence and representing physical measurements, said method comprising the
3 steps of:

4 for each of said plurality of parameters:

5 retrieving an encrypted cryptographic share from a memory
6 location as a function of the sequence of said parameter;

7 decrypting said encrypted cryptographic share with a function of
8 said parameter; and

9 generating a cryptographic key using said decrypted cryptographic shares.

1 35. The method of claim 34 wherein said physical measurements are
2 measurements of DNA.

1 36. The method of claim 34 wherein said function of said parameter used to
2 decrypt said encrypted cryptographic share is a hash function.

1 37. A data structure for use in generating a cryptographic key based on n
2 parameters representing physical measurements, said data structure comprising:
3 n storage locations each associated with a respective one of said n parameters,
4 each particular storage location containing an encrypted cryptographic share which was
5 encrypted using an expected value of a function of the parameter associated with said
6 particular storage location.

1 38. The data structure of claim 37 wherein said function is a hash function.

1 39. The data structure of claim 37 wherein said cryptographic key may be
2 generated using less than n cryptographic shares.